AKAMAI 解决方案简介

借助端到端 Zero Trust 解决方案简化流程、保障安全

Zero Trust 是一种网络安全策略方法，它通过消除用户、设备、网络、数据和应用程序之间的隐性信任来确保企业的安全。 与其他安全解决方案不同， Zero Trust 方法不再假设公司防火墙内的一切都是安全的，而是假设随时可能发生安全漏洞，并对每个访问请求实施最小权限访问，无论该请求来自何处。

为什么 Zero Trust 现在至关重要

对于需要更有效地适应不断变化的现代环境的企业而言，Zero Trust 已成为首选模式。这些企业正在寻找一种新的安全模式，以适应混合工作团队，并保护用户、设备和应用程序（无论其位于何处）。

现代 Zero Trust 架构原则

- 始终根据背景信息明确验证请求
- 明确执行最小权限
- 持续监控

整合是必不可少的

集成式端到端方法

全面的 Zero Trust 方法应覆盖企业的所有实体，包括身份、网络和应用程序。Zero Trust 是一种端到端策略，因此该安全策略需要在所有要素之间实现集成。采用多个松散集成的单点解决方案并不符合这一策略性方法的要求。

Akamai 打造了一套全面而强大的产品组合，可提供现代企业所需的所有 Zero Trust 解决方案。无需安装、运行和修复多种安全产品，相反，企业可以依靠单个供应商来提供所有必要的技术，并享受更低的成本和更高的运营效率。

解决方案之间的信号共享

Akamai 在其 Zero Trust 产品组合中引入了内置自动化，大幅降低了复杂性和定制化需求。这样一来，产品组合中的产品可以在所有产品之间共享威胁情报，进而使每个产品变得更加安全。如果一个产品发现了威胁，其他产品则会获得提醒以抵御威胁。

优势

分布在各处的员工队伍
允许用户在任何地方、任何时间、任何设备上更安全地开展工作

云迁移
提供跨云和混合云环境的安全访问控制

抵御风险
阻止威胁并尽可能减少勒索软件和其他类型恶意软件的横向移动

确保合规性
利用敏感数据周围的微边界，确保合规性

Akamai

全面的端到端产品组合：用户、应用程序和网络

确保工作负载安全

Akamai Guardicore Segmentation：面向应用程序的 Zero Trust

Akamai Segmentation 提供出色的微分段解决方案，旨在限制勒索软件和其他恶意软件的传播。该产品让您可以监测和了解工作负载、流程和应用程序的情况，还可以执行访问策略。

确保网络安全

Enterprise Application Access：Zero Trust 网络访问

Akamai 的 Zero Trust 网络访问技术旨在取代传统的 VPN 技术，以实现强大的用户身份。Enterprise Application Access 不会让整个网络承担风险，而是根据用户为履行职责而需要访问的特定应用程序来允许用户访问。Enterprise Application Access 提供了对用户身份的监测，并且可执行强大的识别和身份验证。

确保用户安全

Secure Internet Access：Zero Trust 互联网访问

Secure Internet Access 是一种基于云的安全 Web 网关解决方案。Secure Internet Access 将检查用户的每一个 Web 请求，并应用实时威胁情报和先进的恶意软件分析技术，以确保只交付安全的内容。恶意请求和内容会被主动阻止。

多重身份验证：强大的 Zero Trust 身份

Akamai MFA 保护员工帐户免受网络钓鱼和其他中间机器攻击。这确保只有经过强身份验证的员工才能访问他们拥有的帐户，其他访问会被拒绝，并可防止员工帐户被接管。

跟踪和监控

搜寻：安全服务

通过采用“始终假设存在入侵”的方法，Akamai 优秀的威胁搜寻团队会不断搜寻异常攻击行为和高级威胁，它们往往能够规避标准安全解决方案的检测。我们的威胁搜寻人员会立即向您告知在网络中发现的任何重大事件，然后与您的团队紧密合作，对相应情况采取补救措施。

Akamai 的优势

Akamai 具有其他 Zero Trust 供应商所没有的优势，并籍此脱颖而出。我们提供广泛的覆盖范围：从传统到现代；从 Windows 到 Linux；从本地到虚拟化；以及容器等。由于我们出色的监测能力，用户可结合全面的背景信息了解各工作负载正在发生的情况。我们优秀的内部威胁搜寻服务可为您的安全团队提供有效助力，让贵公司抢先一步抵御威胁。

如需了解有关 Zero Trust 及如何入门的更多信息，请访问 akamai.com。